



**ORACLE<sup>®</sup>**

## **Future Perfect: New Security Challenges and the Limitations of Technology**

Mary Ann Davidson  
Chief Security Officer

# Background: Evolution of Cybersecurity

- From Maytag repairman to Roto-Rooter
- We all speak cyber now: botnet, rootkit, DDOS, worm, virus, spearphishing...
- Cybersecurity routinely makes MSM front pages
- Cybersecurity is a national security issue
- Government affairs is a full time (tech) job
- Conclusion: expansion of information technology is and should be limited by our ability to manage associated technological risk

# What Do We Mean By Limits?

- Technology cults and false prophets
- Language
- Myopia
- Scale
- Societal values

# Religious Cults and False Prophets

- “Technology is the way, the truth and the life...”
  - Object oriented programming
  - Open source
  - Cloud computing...
- Technology searches for a problem to solve like missionaries search for heathens to convert
  - ,,but businesses want problems solved better, cheaper, or faster than what they are doing now, *without a commensurate increase in risk*
- Non-cult members are often ostracized, ridiculed, shunned, accused of heresy
- Faith != blind faith

# Language

- Technologists often cannot express risks in languages understood by consumers of IT and other stakeholders
  - Users
  - Legislators
  - Business people
- Endless acronym soup: OSCP, IPv6, SOAP, SOA, SAAS, SSL, CVE, CWE, CEE, SITP, HAML, EIEIO...
  - Without the equivalent of the DICNAVAB
- And, we have actual programming languages
  - Incomprehensible to those who don't know them
  - Syntax limits the languages

# Myopia

- Thousands of years of history – tech is a mere blip on the radar screen
- Closed community limits perspective
- Inability to learn lessons from the past
  - Same mistakes, new protocols
  - There are 2 rules for cybersecurity...
- General lack of fertilization from other disciplines
  - History, biology, game theory, economics, finance, engineering, military strategy and tactics...

# Scale

“Assessing the size of the Internet is a somewhat difficult proposition, since it is a distributed body, and no complete index of it exists. What we mean by asking how large the Internet is also plays into how we answer the question. Do we mean how many people use the Internet? How many websites are on the Internet? How many bytes of data are contained on the Internet? How many distinct servers operate on the Internet? How much traffic runs through the Internet per second? All of these different metrics could conceivably be used to address the sheer size of the Internet, but all are very different.” – [www.wisegeek.com](http://www.wisegeek.com)

# Scale, cont'd.

- Financial market meltdown was caused in part by complexity and interdependence
- “Diversification reduces risk, but systemic risk cannot be diversified”
  - ...especially if it is unknown or unacknowledged

# Societal Values

- General lack of societal accountability
  - On the Internet, nobody knows you are a rabid, snarling dog...
- Sound byte/celebrity culture
- Erosion of privacy – sometimes willingly
- Broad embrace of uber connectivity – convenience, productivity, community
- Unwillingness to recognize evil

# Example: The Promise of Smart Grid

- Remote, real-time monitoring of power usage so utilities can better charge for “peak” usage
- Resulting in lower usage, fewer power plants, and “greener” world
- “Do more with less”

# Smart Grid: What We Know

- Plant control systems were not generally designed to be attack resistant because they originally required physical access
  - ...but are now moving to PC- and IP-based systems
  - ...and PDAs can talk SCADA now
- There are cyberattacks with physical consequences (that would be non-recoverable in the short term)
- People designing control systems are not taught defensive programming any more than CS graduates are
- Control systems are being connected to Intranets which are connected to the Internet
- We cannot secure IP-based clients (see “botnets”)
- Smart meters have already been hacked
- Terrorists are targeting the power grid (and seek to acquire more cyberskills)

# Results of (Unchanged) Trajectory

- Widespread embrace of widespread, unmitigateable and systemic risks to critical infrastructure
- Without understanding or acknowledging we are doing it
- With the implicit assumption that “security happens”
- And that technology will someday catch up
- Leading to an increased threat to national security

# How Do We Change the Cybersecurity Future?

- Bind some limits...
  - Religious cults and false prophets
  - Language
  - Myopia
- ...And acknowledge others
  - Scale
  - Societal values
- And reimagine technology



## syn·the·sis

**1 : the combination of parts or elements so as to form a whole;  
*especially* : the production of a substance by union of chemically  
simpler substances**

**2 a : the combining of often very different ideas into an ordered  
whole b : the product so formed**

**(Merriam-Webster)**

# Examples

- Many aspects of art, music, history and other disciplines include synthesis and “borrowed” ideas
  - Music: Jazz, Hawaiian music
  - Language: words, alphabet, idea of writing itself...
  - Economics: relationship between risk/return, Black Scholes model...
  - Art: Impressionism...
  - History: Western civilization...
  - Military history/strategy: force multiplier, energy maneuverability theory (OODA), defense in depth
  - Nuclear strategy, biology: game theory

# Why Court Synthesis?

- “There is nothing new under the sun” (Ecclesiastes)
- Synthesizing ideas, canons, patterns from other disciplines
  - Help recognize old problems in new guise
  - Apply old solutions to new problems
  - Explain technology in terms others can understand because they are familiar patterns or stories
  - Deprogram cult members
- Occasionally, start a revolution (e.g., OODA loop)

# Synthesis Applied to Cybersecurity

- Military History, Strategy and Tactics
- Biology
- Economics

# Synthesis: Applicability of Military Constructs to IT

- Implications of a networked battlespace
- Requirement for situational awareness
- Marine Corps ethos
- E-M theory

# “The Network is the Battlefield”

- DoD’s Global Information Grid vision: combine physically separate networks to increase timeliness of information to the war fighter
  - ...thus eliminating several natural defensive boundaries
  - ...and forcing defense of the entire network
  - ...leading to Isandlwana, not Rorke’s Drift?
- As war fighting increasingly relies upon an IT backbone, the network itself becomes the battlefield
  - Superior force-of-conventional-arms – hard to get
  - Superiority of cyber-arms – much easier
  - Goal: disrupt our ability to wage war
- Desire for benefit means embracing asymmetric risk, because benefits seem clear ... but risks aren’t

# ...Which May Favor Our Adversaries

- Technology is a *force multiplier*, but could over reliance upon it be an Achilles' backbone?
  - Warfare has become information-centric
  - “Where there is capability, an enemy may develop intent”
- Little to no situational awareness
  - Who is on the network?
  - Friend or foe?
  - What is on the network?
  - What is my state of “mission readiness”?
  - What's over the hill?

“He who defends everything defends nothing.” – Frederick II

# Required: Self-Awareness of the Network

- Lack of situational awareness is caused by lack of basic information
  - No standards for what am I running, in what state...
  - No standards for what audit records are collected or format
- Current limitations
  - SIM vendors can't correlate non-existing data
  - Value add is the BI component, not “translation services”
- Government could promote and enforce standards as a public good
  - Example: Transcontinental Railroad
  - Example: SCAP

# E-M Theory: Will It Work On Networks?

- Fighter pilots “win” based on agility (Boyd’s energy-maneuverability (E-M) theory)
- OODA (observe, orient, detect, act)
  - OODA was an air warfare concept that changed the face of war (notably in Gulf War I)
  - And has been applied to other disciplines
  - Is there applicability to cyber-offense and defense?
    - If targets are not static but evolving, it might

# Required: Innate Defensibility of Software

- “Every Marine a rifleman...”
  - Products must self defend
  - All of them
- All territory is not equally important, and you will take casualties
- “Dynamic redoubts”
  - Active - not passive - defense, including adaptive defense

# Synthesis Applied to IT Security

- Military History, Strategy and Tactics
- **Biology**
- Economics

# A Few Biological Concepts

- “Biological diversity” as a defense mechanism
  - Irish potato famine argument against monoculture (Giffen good?)
- Viruses
  - Use the host but don’t generally kill it
  - “Antibodies” = virus signature
  - Adaptive viruses (flu, rhinovirus) more long-lived than static ones
- “Roundup ready” weeds
- Trees “signaling” they are under attack

# And Their IT Counterparts

- “Monoculture” argument for IT systems
  - Countered by economic arguments of total cost of ownership
- Viruses
  - Could hosts’ defensibility also “spread” (e.g., SCAP)
- How adaptive, automated and rapid can defenses be made (OODA considerations)?

# Synthesis Applied to IT Security

- Military History, Strategy and Tactics
- Biology
- **Economics**

# Synthesis: Applicability of Economic Constructs to IT

- Opportunity cost
- Cost avoidance
- Net Present Value
- Portfolio theory
- Efficient markets/market failures
- Externalities/social costs

# Economics for IT Vendors

- Cost avoidance of building security in (and avoiding defects) is huge
  - Increases with maturity of product (number of versions, platforms, interdependencies of products)
  - Software development in large firms is “process manufacturing”
- Opportunity cost is also high
  - “With same people you use on bug-fixing, you could build a new product”
- Net present value (NPV)
  - Discounted value of defect avoidance in today’s dollars

# Economics for IT Vendors (cont'd)

- Portfolio theory
  - Diversification reduces risk
  - But market risk is non-diversifiable

# The Problem of Residual Risk

- Scale
  - “Known unknowns” and the problem of complexity
- Societal values
  - Privacy, freedom, security – pick 2 out of 3
  - The Oregon Trail and the Interstate
- And reimagine technology
  - John Boyd’s legacy

# Conclusions

- We need to change the way we think about, imagine, talk about, and explain cybersecurity
- Technology is not salvation: it's a tool
- We can change the world
  - Through technology
  - By changing how we think about it
  - By limiting how we use technology

# Resources

- *How Markets Fail* by John Cassidy
- *War Made New* by Max Boot
- *Carnage and Culture* by Victor Davis Hanson
- *Guns, Germs and Steel* by Jared Diamond
- *The Botany of Desire* and *The Omnivore's Dilemma* by Michael Pollan
- *Boyd: The Fighter Pilot Who Changed the Art of War* by Robert Coram
- *Prisoner's Dilemma* by William Poundstone

# Resources, cont'd.

- Richard Thieme: <http://www.thiemeworks.com/>
- Dan Geer: [http://en.wikipedia.org/wiki/Dan\\_Geer](http://en.wikipedia.org/wiki/Dan_Geer)



**"A nation, as a society, forms a moral person,  
and every member of it is personally responsible  
for his society."**

**-Thomas Jefferson  
(in letter to George Hammond, 1792)**



**ORACLE IS THE INFORMATION COMPANY**